



CVE-2023-25579

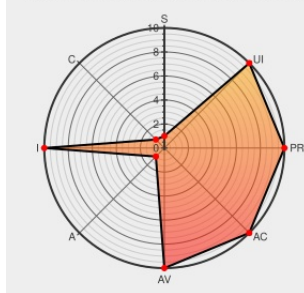
Published on: Not Yet Published

Last Modified on: 03/03/2023 03:09:00 PM UTC

CVE-2023-25579 - advisory for GHSA-273v-9h7x-p68v

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N



Certain versions of [Nextcloud Server](#) from [Nextcloud](#) contain the following vulnerability:

Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Folder::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue.

CVE-2023-25579 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [nextcloud](#) - **security-advisories** version = < 23.0.12

Affected Vendor/Software: [nextcloud](#) - **security-advisories** version = >= 24.0.0, < 24.0.8

Affected Vendor/Software: [nextcloud](#) - **security-advisories** version = >= 25.0.0, < 25.0.2

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVE References

Description	Tags	Link
Potential directory traversal in OC\Files\Node\Folder::getFullPath · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	MISC github.com/nextcloud/security-advisories/security/advisories/GHSA-273v-9h7x-p68v
Make sure that path is normalized and then checked, by come-nc · Pull	github.com	MISC github.com/nextcloud/server/pull/35074

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextcloud	Nextcloud Server	All	All	All	All
Application	Nextcloud	Nextcloud Server	All	All	All	All
cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:*:*:						
cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:enterprise:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-25579 : Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Fold... twitter.com/i/web/status/1...	2023-02-22 19:08:31
 /r/netcve	CVE-2023-25579	2023-02-22 22:54:53

← Previous ID

Next ID →

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)